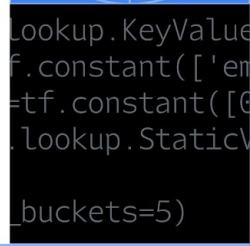
Google Developer Groups

CyberSec Bootcamp Lecture – 0x05



Google Developer Groups

MEET YOUR GUIDES

Zishan Ansari

(Mentor)

CyberSec - GDG

LinkedIn

GitHub

Google Developer Groups

MEET YOUR GUIDES :

Rohit Choudhary

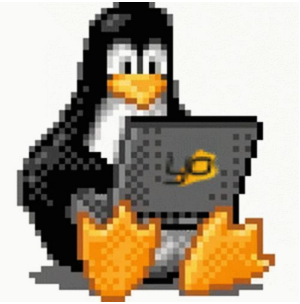
(Instructor)

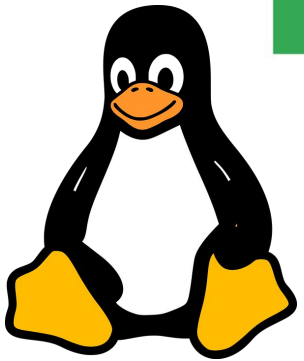
CyberSec - GDG

LinkedIn

GitHub

Google Developer Groups



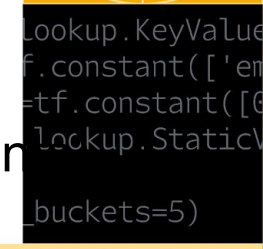


Linux Logging & becoming anonymouse

Google Developer Groups

Understanding Linux Logging

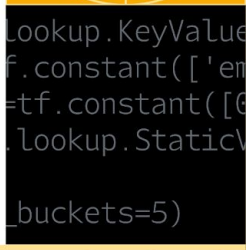
- Why logging is important.
- Common use cases: system performance monitoring, debugging, security auditing.
- Brief explanation of what logs are (records of system even



Google Developer Groups

Classification of Linux Logs

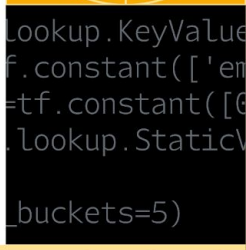
- System logs: Kernel messages, system events (`dmesg`, `/var/log/syslog`).
- Application logs: Logs specific to software (e.g., Apache, NGINX).
- Security logs: Authentication attempts (`auth.log`, `secure`).
- Audit logs: Compliance tracking, auditd logs.
- Example paths: `/var/log/messages`, `/var/log/kern.log`.

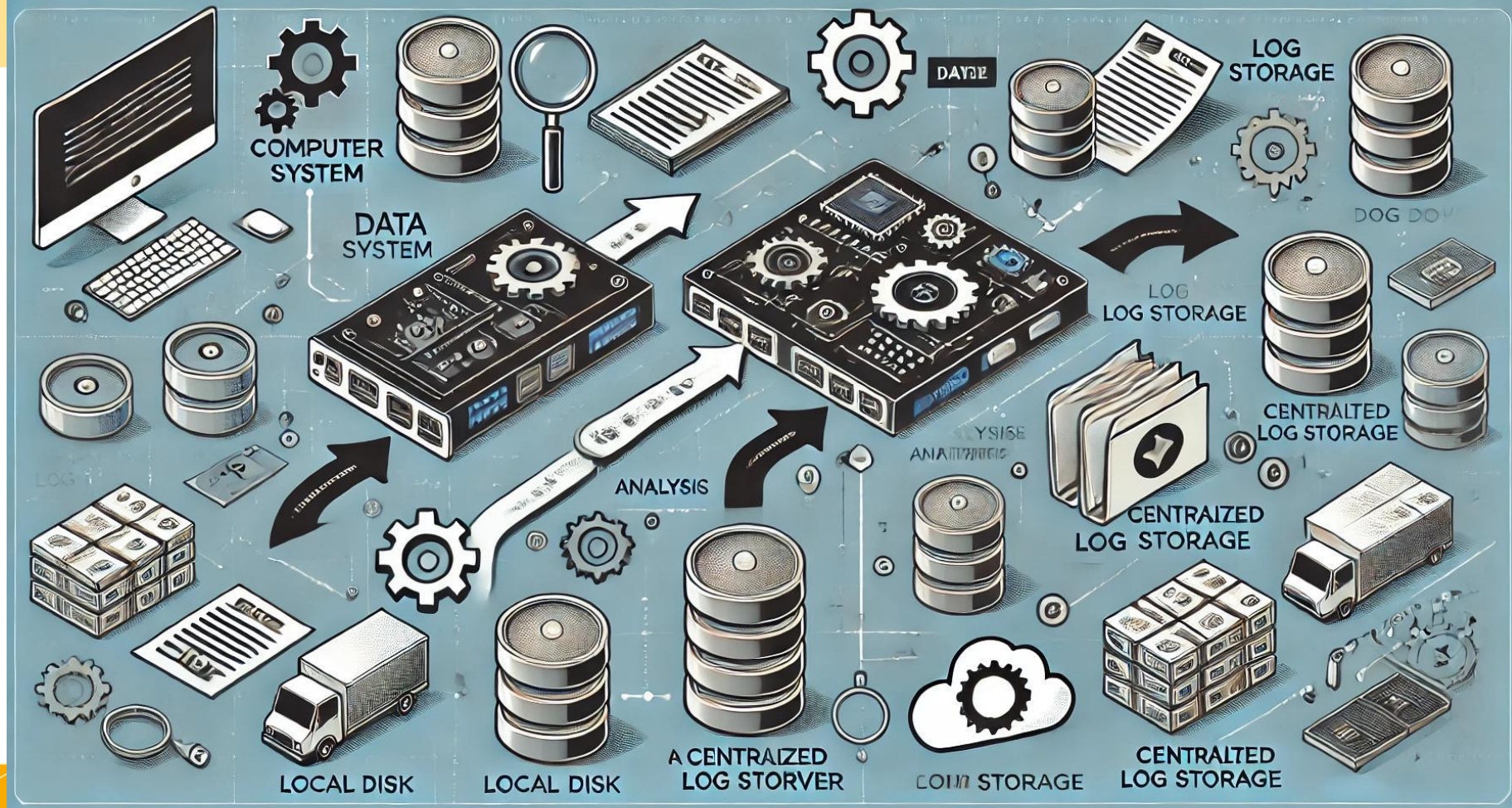


Google Developer Groups

Linux Logging Architecture

- Overview of logging daemons (`syslogd`, `rsyslogd`, `journald`).
- Interaction between applications and log files.
- Key directories: `/var/log/`.

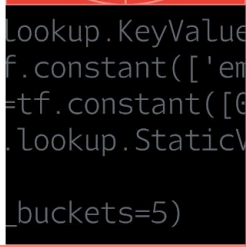



COMPUTER SYSTEM
DATA SYSTEM
LOG STORAGE
LOG STORAGE
CENTRALTED LOG STORAGE
CENTRAIZED LOG STORAGE
ANALYSIS
LOCAL DISK
LOCAL DISK
A CENTRAIZED LOG STORVER
CENTRALTED LOG STORAGE

Google Developer Groups

The Syslog Protocol

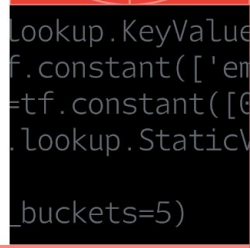
- Components: Facilities (auth, mail, daemon), severity levels (info, error).
- Example syslog message format.
- Explain priority values (e.g., `<priority> = facility * 8 + severity`).
- Example log message: `Oct 3 14:05:22 hostname process[1234]: Error message`.



Google Developer Groups

Modern Logging with Journald

- Features: binary storage, metadata-rich logs.
- Configuration: persistent logs in `/var/log/journal`.
- Basic commands:
- `journalctl` overview.
- Filtering by unit (`journalctl -u service_name`).
- Time filtering (`journalctl --since "2025-01-01"`).

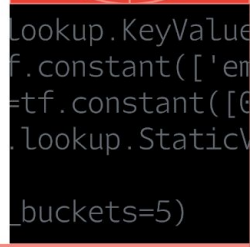


Google Developer Groups

Configuring Logging Systems

Rsyslog: Use of `/etc/rsyslog.conf` for filtering, forwarding.
Journald: Key options in `/etc/systemd/journald.conf`.
Examples:

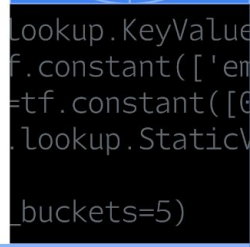
- Setting log file size limits.
- Configuring log rotation.



Google Developer Groups

Analyzing and Monitoring Logs

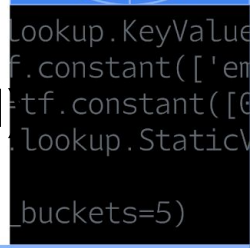
- Tools:
  - `grep` and `awk` for log parsing.
  - `tail -f` for real-time monitoring.
- Example command outputs.
- Highlight best practices for searching logs efficiently.



Google Developer Groups

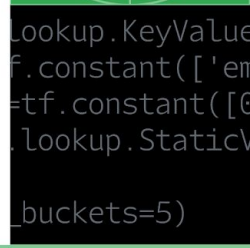
Ensuring Log Security

- Restrict access using file permissions (`chmod`, `chown`).
- Encrypt sensitive logs with GPG or encryption frameworks.
- Tools for monitoring unauthorized access to log files (e.g., auditd)



Google Developer Groups

Becoming Secure and Anonymous on the Internet



Google Developer Groups

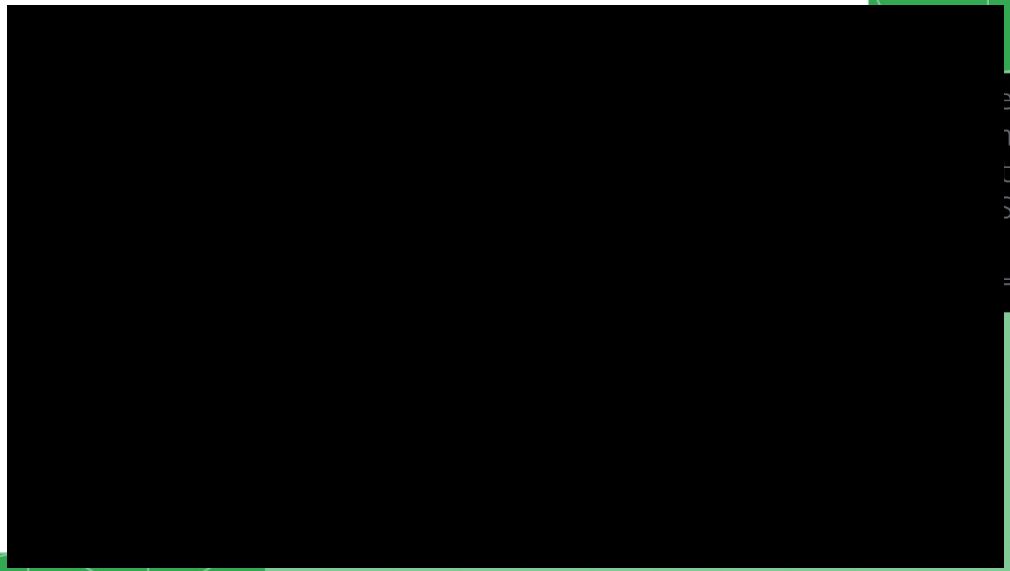
Introduction to Internet Tracking and Privacy

- Online activities are being tracked by companies and government agencies.
- Hackers and individuals must understand how to minimize tracking.
- Methods to improve online anonymity and security.

Google Developer Groups

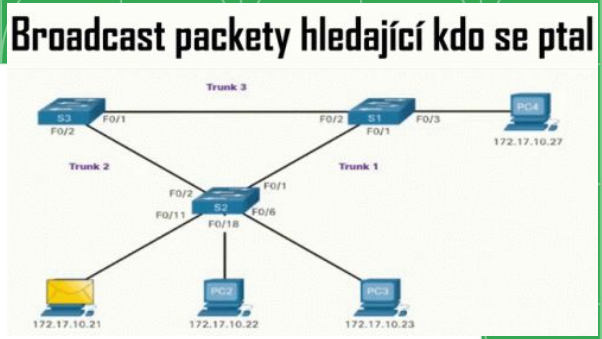
Methods for Online Anonymity

- The Onion Network (Tor)
- Proxy Servers
- Virtual Private Networks (VPNs)
- Private Encrypted Email



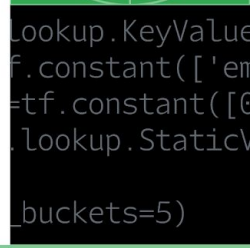
Tails

Google Developer Groups



How the Internet Tracks Our Activities

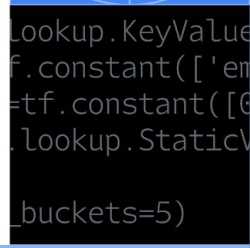
- Your IP address reveals your identity and location.
- Websites and services (e.g., Google) track your online activities.
- Data packets contain your IP address and routing information.



Google Developer Groups

Understanding Traceroute

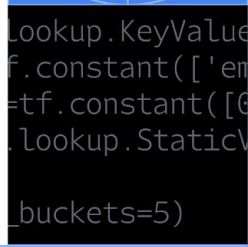
- `Traceroute` shows the path data takes across the internet.
- Helps visualize how your IP address is exposed.
- Example: A traceroute to Google (mention number of hops).



Google Developer Groups

The Onion Router (Tor) Network

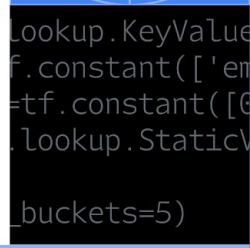
- Developed for anonymous communication by the U.S. Navy.
- Data travels through 7,000+ volunteer-run routers globally.
- Each hop encrypts and decrypts data to protect anonymity.
- **Security Note:** Mention that Tor has been compromised in the past by agencies like NSA.



Google Developer Groups

Using the Tor Browser

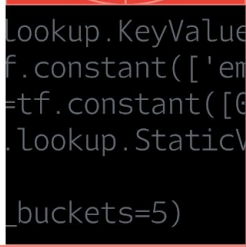
- Download and install from the official Tor Project website.
- Provides access to both the regular and dark web.
- Trade-off: Slower browsing speed due to network encryption.



Google Developer Groups

Proxy Servers

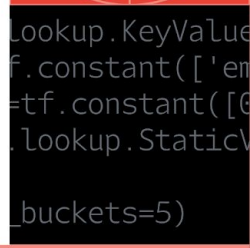
- A proxy acts as an intermediary between the user and the internet.
- The proxy server replaces your IP address with its own.
- Proxy chains can increase anonymity by using multiple proxies.



Google Developer Groups

Using Proxychains in Kali Linux

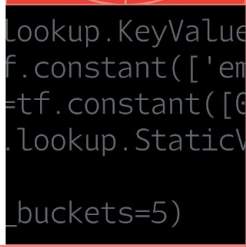
- Proxychains can route traffic through multiple proxies.
- Example command: `proxychains nmap -sT -Pn <IP address>`
- Configuration via `/etc/proxychains.conf` file.



Google Developer Groups

Configuring Proxychains

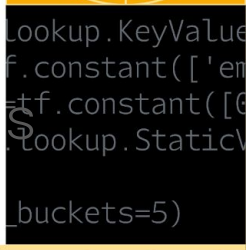
Modify the `proxychains.conf` file to add proxies.
Use dynamic or random chaining to enhance anonymity.
Proxy chaining can be configured to select proxies automatically.



Google Developer Groups

Security Considerations with Proxies

- Avoid free proxies for serious anonymity, as they may log your data.
- Paid, trusted proxies are safer for privacy.
- Understand the limitations of proxies, especially with government surveillance.



Google Developer Groups

conclusion

- Multiple methods exist to secure your online activities.
- Tor, proxy servers, VPNs, and encrypted emails help protect privacy.
- Always be aware of the limitations and potential risks.